Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A wireless communication device arranged and constructed to enable a function when an identity of a user is confirmed, the wireless communication device comprising:

a plurality of biometric devices, each of the plurality of biometric devices for assessing the identity of the user; and

a controller, coupled to the plurality of biometric devices, for selecting one of the plurality of biometric devices when a corresponding predetermined condition is present,

wherein the corresponding predetermined condition comprises one of a time of day, a date, an interval, and situation circumstances and wherein the situation circumstances comprise one of ambient light, temperature, and ambient noise and a corresponding biometric sensor comprises, respectively, a camera, a skin sensor, and a microphone;

wherein the controller enables the function when the identity of the user is confirmed by the one of the plurality of biometric devices.

2. (Original) The wireless communications device of claim 1 wherein:

the function comprises one of access to the wireless communication device, a feature, a content, an application, and a service provided by the wireless communication device.

3. (Original) The wireless communications device of claim 1 wherein the plurality of biometric devices comprises a sensor for one of fingerprint recognition, hand recognition, retinal scan, iris recognition, signature recognition, face recognition, and voice recognition.

4. (Cancel)

5. (Cancel)

6. (Currently amended) ~~The wireless communications device of claim 1~~ A wireless communication device arranged and constructed to enable a function when an identity of a user is confirmed, the wireless communication device comprising:

a plurality of biometric devices, each of the plurality of biometric devices for assessing the identity of the user; and

a controller, coupled to the plurality of biometric devices, for selecting one of the plurality of biometric devices when a corresponding predetermined condition is present;

wherein the controller enables the function when the identity of the user is confirmed by the one of the plurality of biometric devices; wherein a first biometric device has a higher

reliability in assessing the identity of the user and is selected when the corresponding predetermined condition indicates a suitable operating environment.

7. (Original) The wireless communication device of claim 1 wherein the user may override the controller selection of one of the plurality of biometric devices and select a second biometric device to confirm the identity of the user.

8. (Currently amended) ~~The wireless communications device of claim 1~~ A wireless communication device arranged and constructed to enable a function when an identity of a user is confirmed, the wireless communication device comprising:

a plurality of biometric devices, each of the plurality of biometric devices for assessing the identity of the user; and

a controller, coupled to the plurality of biometric devices, for selecting one of the plurality of biometric devices when a corresponding predetermined condition is present;

wherein the controller enables the function when the identity of the user is confirmed by the one of the plurality of biometric devices and wherein the controller is operable to limit a number of times a second biometric device may be used to confirm the identity of the user before a first biometric device must be used to confirm the identity of the user.

9. (Original) The wireless communication device of claim 1 where the one of the plurality of biometric devices is selected from a list that is arranged hierarchically according to a characteristic of the each of the plurality of biometric devices.

10. (Original) The wireless communication device of claim 9 wherein the characteristic for arranging the list is one of an ease of confirming the identity of the user and a reliability of confirming the identity of the user.

11. (Original) The wireless communication device of claim 1 further comprising:

a keypad for entering a password when none of the plurality of biometric sensors is selected,

wherein the controller is operable to enable the function when the password matches a known password.

12. (Currently amended) A system for authorizing the use of a feature on a wireless communication device comprising:

a plurality of biometric sensors, each for collecting a sample corresponding to a user biometric; and

a controller coupled to the plurality of biometric sensors for:

collecting a first sample from one of the plurality of biometric sensors, the one of the plurality of biometric sensors selected when a corresponding predetermined condition is present; and

authorizing the use of the feature when the first sample corresponds to a known sample, wherein a first biometric sensor must be used to authorize the use of the feature after a predetermined number of consecutive uses of a second biometric sensor to authorize the use of the feature.

13. (Currently amended) The system of claim 12 wherein the one of the plurality of biometric sensors ~~sensor~~ comprises a sensor for recognition of one of a fingerprint, a hand, a retina, an iris, a signature, a face, and a voice.

14. (Currently amended) The system of claim 12 further comprising a ~~first~~ biometric sensor selected by the controller according to the corresponding predetermined condition and ~~a second~~ an other biometric sensor selected by the user, wherein the user overrides the controller and the first sample is collected from the ~~second~~ other sensor.

15. (Cancel)

16. (Original) The system of claim 12 wherein the feature comprises one of a local function supported on the wireless communication device and a remote function accessed via a network.

17. (Currently amended) A method for enabling a feature on a wireless communication device comprising:

collecting a biometric sample corresponding to a user from one of a plurality of biometric sensors, the one of the plurality of biometric sensors selected when a corresponding predetermined condition is present; and

enabling the feature when the biometric sample corresponds to a known sample,

wherein the collecting further comprises:

selecting a first biometric sensor when a predetermined condition is present, the predetermined condition indicating a suitable operating environment for the first biometric sensor, thereby resulting in more accuracy when matching the biometric sample to the known sample..

18. (Currently amended) The method of claim 17 wherein collecting the biometric sample further comprises:

evaluating [[a]] the predetermined condition corresponding to one of the plurality of biometric sensors;

selecting one of the plurality of biometric sensors when the predetermined condition exists; and

collecting the biometric sample using the one of the plurality of biometric sensors.

19. (Original) The method of claim 18 wherein enabling the feature further comprises:

enabling the use of the feature using one of a password and a token when the predetermined condition is not present.

20. (Original)The method of claim 19 wherein the using the token further comprises using one of a smart card, a magnetic stripe card, a radio frequency tag and a key.

21. (Cancel)

22. (Original) The method of claim 17 wherein the collecting further comprises:

selecting the one of the plurality of biometric sensors using a preferred order corresponding to one of accuracy of collecting the biometric sample and ease of collecting the biometric sample.

23. (Currently amended) The method of claim ~~21~~ 17 wherein the predetermined condition includes an uncertainty parameter for selecting a second biometric sensor even when all other of a plurality of predetermined conditions are present.

****